REMARKS

In the Office Action dated July 31, 2002, the previously-made restriction requirement was reiterated. As noted in the Office Action, Applicants have previously elected claims 1-9 for examination, and Applicants herewith affirm that election. Accordingly, non-elected claims 10-16 have been canceled.

Claims 1-9 were rejected under 35 U.S.C. §103(a) as being unpatentable over French in view of Emmett et al. This rejection is respectfully traversed for the following reasons.

The subject matter of dependent claim 2 has been embodied in independent claim 1 and claim 2 has been canceled. Additionally, claim 1 has been amended to include the step of storing security-relevant data in a security module and inserting the security module on a device motherboard, as an affirmatively-claimed method step. Although this step was contained in the preamble of claim 1 as originally filed, the Examiner may have felt justified in not giving this part of the claim patentable weight, since it was only set forth in the preamble. Since this step is now included as an affirmatively-claimed step of the method of claim 1, it must be given patentable weight. The step of storing security relevant data in a security module is relevant to the patentability of claim 1 in view of the Examiner's reliance on the French reference, which is not directed to a device for protecting security data stored in the security module itself. The Emmett et al reference, of course, discloses the storage of security data in a security module of a postage meter device, however, in view of the absence of such storage in the French reference, and particularly in view of the absence of any need to store security data in a module in the French reference, Applicants respectfully submit that a person of ordinary skill in the art seeking to design a postal security module has no basis whatsoever to consult a reference such

as the French patent, which does not in any way relate to the storage and/or protection of security data. If there is any information disclosed, or made use of, in the system described in the French patent, it is the encoding information which is contained in the key which must be inserted in the device for arming and disarming. Although encoded data may be considered to be "stored" in such a key, such data are not stored in the security device itself, and therefore there is no need to provide measures in the device itself to protect that data.

This is also relevant to the overall intended use of the French device, which is for the purpose of protecting another device from theft (namely a radio) rather than to protect data in the security module itself. Moreover, as the Examiner has noted, the intended purpose of the French device is to render the usage of the overall device (i.e. the radio) useless if the radio with the security device is removed from a vehicle. This is opposite to the intended purpose of the security module disclosed and claimed in the present application. Although the security module is certainly intended to render itself useless by erasing the security data, if it is improperly used or improperly removed from the motherboard, the present inventors have recognized that legitimate situations occur wherein removal of the security module is proper, such as for temporary removal from the motherboard while the motherboard is being repaired, or for transferring the security module to another motherboard if the motherboard on which it is currently inserted catastrophically fails so that this motherboard cannot be used any more.

In such situations, the purpose of the security module disclosed and claimed in the present application would be defeated if it could not be re-initialized for usage after the motherboard is repaired, or after placement on a different motherboard. Claim 2 of the original application was directed to steps for allowing such re-

initialization and such (proper) re-use, and that subject matter has now been embodied in independent claim 1.

As the Examiner noted, the Emmett et al reference mentions the well-known feature in the context of postal security devices of causing erasure of security data contained in the security module if the module is tampered with. The Emmett et al reference, however, is not concerned with the problem, and therefore provides no teachings, of what happens to the security data if the module is legitimately removed from its motherboard.

More importantly, for the reasons noted above there are no security data stored in the device in the French reference, and therefore the mere fact that the Emmett et al reference teach the well known step of erasing stored security information upon evidence of tampering does not provide a person of ordinary skill in the art in the design of security modules with any useful information for modifying the French device. As noted above, an insertable key carries the only encoded information for which use is made in the French device, and therefore even if a person of ordinary skill in the art had knowledge of the teachings of Emmett et al, the ability to erase security information would be unavailing in the French reference, since there is no way to "erase" the encoded information contained in the key used in the French device.

Moreover, the ability to reinitialize the security module for subsequent proper usage after it has been removed from its original insertion location on the motherboard is made possible in the subject matter disclosed and claimed in the present application by dividing the relevant functions between the first function unit and the second function unit. The first function unit not only serves as a status monitoring and indicating unit, but also serves as the unit which allows re-

initialization of the second functional unit if and when the security module has been properly removed from the motherboard. Since the second functional unit is intended to erase the security data if the security module is removed from the motherboard, this function would be compromised if the second function unit were able to re-initialize itself, since the second functional unit would then have no way to "know" whether the removal from the motherboard was proper or improper. By using the first function unit to "inform" the second function unit if and when removal was legitimately undertaken, the security module can be removed and subsequently re-initialized as needed for legitimate purposes. There is no indication that the French reference, even if modified in accordance with the teachings of Emmett et al, would allow re-use of the radio under any circumstances, after it has been removed from the vehicle. Although the French patent is silent on this point, presumably if the removed radio were recovered and were re-installed in the vehicle, it would be necessary to re-equip the radio with a new security module.

For all of the above reasons, Applicants respectfully submit that a person of ordinary skill of the art of security module design would have no basis to consult the French patent, and would have no motivation or inducement to modify the French patent in accordance with the teachings of Emmett et al. Moreover, even such a modification were made (for reasons unknown to the present Applicants), a method as set forth in claim 1 still would not result.

Claims 3-9 add further steps to the non-obvious method of claim 1, and are therefore submitted to be patentable over the teachings of French and Emmett et al for the same reasons discussed above in connection with claim 1.

All claims of the application are therefore submitted to be in condition for allowance, and early reconsideration of the application is respectfully requested.

Submitted by,

Steven N. Noll (Reg. 28,982)
SCHIFF, HARDIN & WAITE
CUSTOMER NO. 26574
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Applicants.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

Claim 1 has been amended as follows:

1. (Amended) A method for protecting a security module[, in which security-relevant data are stored, inserted on a device motherboard,] comprising the steps of:

storing security relevant data in a security module and inserting said security module in a device motherboard;

monitoring proper insertion of said security module on said device motherboard with a first function unit and a second function unit in said security module;

signaling at least one security-related status of said security module with said first function unit; [and]

detecting at least one of improper use and improper replacement of said security module with said second function unit and, upon a detection of at least one of said improper use and said improper replacement, said second function unit causing said security-relevant data to be erased[.];

following at least one of proper u se and proper replacement of said security module, re-initializing, with said first function unit, any erased, security-relevant data; and

after said re-initializing, enabling each of said first function unit and said second function unit to re-commission said security module.